Samleikin Registration Authority Policy (RAP)

Version 1.1. - 09.06.2021

Change Log

Version	Change Date:	Valid from	Author:	Change:
0.9	01.04.2020		Jósup Henriksen	Created first version with version control
1.0	01.05.2020		Jósup Henriksen	Policy approved by Gjaldstovan TSP Management Board
1.1	17-03-2021	09-06-2021	Jósup Henriksen	Policy approved by Gjaldstovan TSP Management Board 7th of May 2021. 1.3 - TSP mgmt board mail adr changed from tsp@gjaldstovan.fo to 1881@talgildu.fo 2.1.2 - Link to terms and conditions inserted. Was missing before

1. Introduction

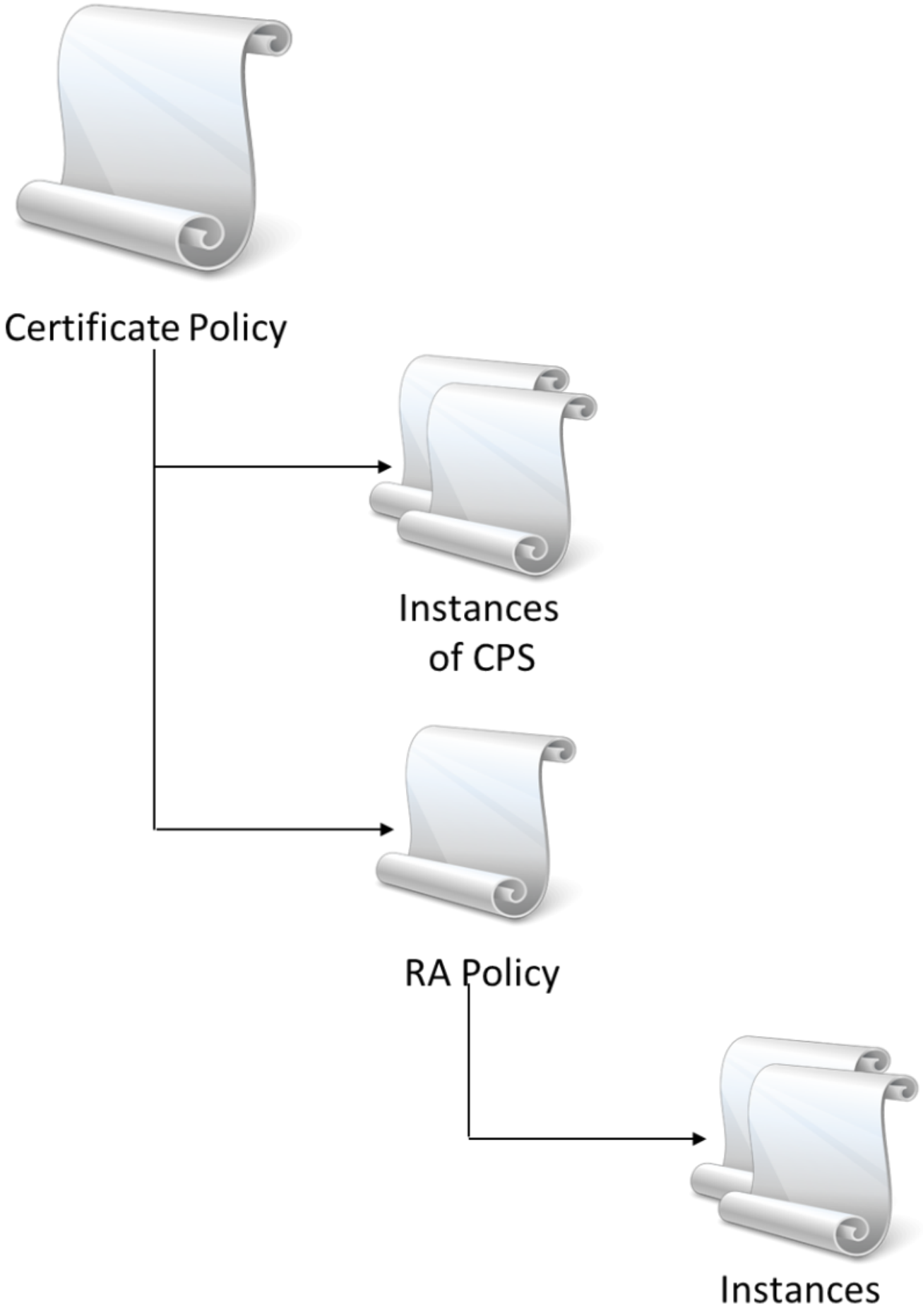
This RAP is owned and maintained by the Gjaldstovan TSP Management Board.

This document defines Samleikins Registration Authority Policy that serves as the foundation for RA organizations that are allowed to operate within the nat ional Faroese eID programme Talgildur Samleiki (shortened "Samleikin").

This Registration Authority Policy (RAP) is governed by each Certificate Policy, CP, that apply to certificates that are enrolled. No RA operations shall conflict with the regulations of the CP and practice statements, CPS, employed by the CAs that issue certificates within Samleikin. Also, every RA organization have to develop and maintain a practice statement that describes how the RA organization is implemented and how requirements from this RAP are fulfilled. Every such Registration Authority Practice Statement (RAPS) have to be approved by Gjaldstovan before any RA organization is allowed to operate within Samleikin. Also revisions to approved RAPSes must be approved by the Gjaldstovan TSP Management Board before it is allowed to be put in effect. Also all RAs are obligated to ensure that sufficient, monetary and personnel, resources are allocated in order to meet the requirements of its RAPS and fulfill all its obligations according to this RAP.

1.1. Overview

An overview of --the policy structure is shown in the diagram below. At the top of the hierarchy is Gjaldstovan TSP Management Board that owns and maintains and sets out the policies under which Samleikin participants must comply with.


Certificate Policy
Instances
of CPS
RA Policy
Instances

Registration Authorities (RAs) are entities that authenticate certificate requests within Samleikin. Only RA organizations that have been authorized by a signed agreement with the Gjaldstovan TSP Management Board can act as RAs.

This RAP describes the procedures and routines that are applied when issuing certificates within Samleikin for:

- Physical persons (Certificate Holders that are End-Users)
- LRA Manager certificates (Management CA certificates for RA persons)
- LRA Certificates (Management CA certificates for RA persons)
- Local Supporter certificates (Management CA certificates for RA persons)
- Internal auditor (Management CA certificates for RA persons)

RAs that operate within Samleikin must adhere to this RAP and create and maintain a RAPS that is approved by the Gjaldstovan TSP Management Board. An RA without approved RAPS will not become a part of Samleikin.

1.2 Document name and identification

The identifier for this RAP is:

- Samleikin Registration Authority Policy

OID for this RAP is: 1.2.208.189.1.1.11

1.3 Policy administration

This RAP is administered by Gjaldstovan TSP Management Board that can be reached on the following address:

Gjaldstovan
Kvíggjartún 1
160 Argir
Faroe Islands

Gjaldstovan can also be contacted by email on the following address: 1881@talgildu.fo

2. Terms and obligations

2.1 Obligations

2.1.1 RA obligations in relation to CAs

RAs in accordance with this RAP must:

1. Operate within the obligations stipulated by this RAP
2. Conduct audits in accordance with this RAP, regarding internal and external audits
3. Conduct Certificate Holder identification in accordance with this RAP
4. Suspend and/or revoke certificates in accordance with this RAP
5. Gather and verify information that are part of certificates
6. Deliver private keys to Certificate Holders when applicable in accordance with this RAP
7. Deliver key bearing tokens to Certificate Holders when applicable in accordance with this RAP
8. Archive information in accordance with this RAP
9. Verify that certificates only contain information as regulated by the certificate profiles supported by the issuing CAs
10. Ensure that rules for certificate applications are enforced as specified in this RAP
11. Meet operational requirements as specified by this RAP

2.1.2 Certificate Holder obligations

Certificate Holder obligations are stipulated by the applicable Terms and Conditions. These are available at: https://repository.samleiki.fo/terms-and-conditions-en.html

Rules and routines that shall be part of RAPS

The following rules and routines shall be documented and governed for each RA by means of its RAPS.

1. Routines for issuance, revocation and Certificate Holder acceptance of certificates.
2. Rules for verification of Certificate Holder information
3. Background checks of RA-personnel
4. Archiving of information according to the stipulations of this RAP
5. Compliance audits in accordance with this RAP
6. Disaster recovery plans

2.2 Responsibilities

2.2.1 RA responsibilities within its operating boundaries

RAs are responsible for the following within its operating boundaries:

1. That the requirements and specifications of this RAP are fulfilled
2. That periodic controls and audits are conducted, regarding proper issuance and usage of issued certificates
3. That archiving is conducted in accordance with this RAP

2.2.2 RA responsibility disclaimers

RAs are not responsible for consequences or damage due to:

1. That keys are used in violation to the Terms and Conditions
2. That Certificate Holders use certificates in violation to the Terms and Conditions
3. Errors caused by CAs
4. Errors caused by other RAs

2.3 Financial responsibilities

RA is required to demonstrate that they have the financial resources necessary to discharge their obligations under this RAP and any other relevant and associated documentation, e.g. RAPS, or agreement.

2.4 Governing law

Subject to any limits appearing in applicable law, the laws of the Faroe Islands shall govern the enforceability, construction, interpretation, and validity of this RAP. If a dispute cannot be settled by conciliation, either of the parties may choose to bring the dispute before the ordinary courts. The venue is Føroya Rættur, Tórshavn. The applicable law is Faroese law.

2.5 Fees

RAs are allowed to charge the Certficate Holders for specific RA related services after approval of the Gjaldstovan TSP Management Board. This must be described in the RAPS of RA organizations.

2.6 Compliance audit and other assessments

RAs shall continuously conduct audit reviews in order to make sure that this RAP is correctly implemented. Such audits shall at least occur once on a yearly basis or when suspicious activities are detected within a RA operating boundary. When flaws or a need for change in the implementation of the RAP arise, RAs shall take appropriate action in order to remediate such situations by changing routines and or initiate changes to its RAPS. Changes to this RAP are managed by the Gjaldstovan TSP Management Board. If changes to this RAP affect the security level of Samleikin, a new policy with a new OID is to be established to reflect this change in security level.

2.7 Confidentiality

Confidentiality concerning information for Certificate Holders is stipulated by the following laws:

- Dátuverndarlógin
- Fyrisitingarlógin
- Lóg um talgildan samleika

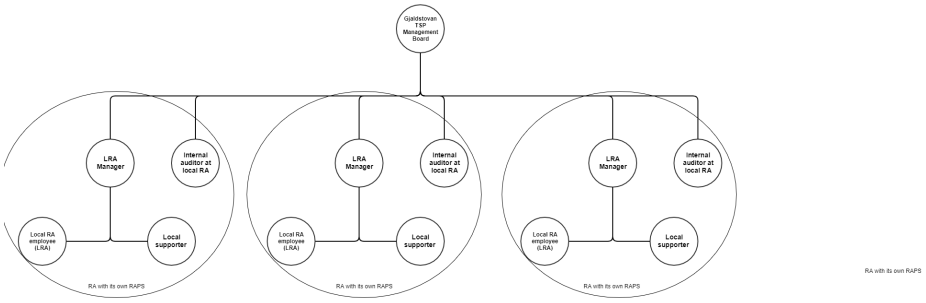
All RA operations must meet the requirements of Faroese law and the stipulations within this RAP and any CP associated with issued certificates.

2.8 Terms and agreements

All RAs operating within Samleikin shall sign a formal agreement with the Gjaldstovan TSP Management Board that dictates RA operating responsibilities and requirements. Such agreements also dictate that RAs shall abide under the stipulations of the CPs associated with issued certificates. To every such agreement a RAPS shall also be appended, that describes the local implementation of this RAP.

3. Roles & Responsibilities

The hierarchy of roles regarding the RAs that operate within Samleikin is as follows:



In order to discharge the responsibilities delegated from the Gjaldstovan TSP Management Board in relation to RA-activity there are requirements each RA organization must meet in relation to roles and responsibilities within the local organization. In every RA there must be only the following roles:

3.1 LRA manager

The LRA Manager is responsible for running the governance of the RA in the organization. As such they must agree and sign off on local operational processes and should assure themselves regularly that these processes are being adhered to. The LRA manager is responsible for assigning and maintaining every other role holder within its RA-organization, maintaining the RAPS of the RA-organization, be able to lead the daily work and be comfortable with every RA-persons actual work and the tools they use. The LRA manager must ensure the effective training of every RA-person within their organization.

LRA manager responsibilities
Responsible for running RA-governance in his organization
Responsible for the development and maintenance of a RAPS that meet the demands in this RAP
Make sure the RA-organization is adequately staffed
Train RA-persons and ensure they are competent to carry out their roles and adhere to policy and processes
Ensure that the access control to RA-facilities is in order and up to date
Ensure that the RA-organization is audited as required by the Gjaldstovan TSP Management Board
Ensure withdrawn employees from the RA-organization have their access rights removed in a timely way
Responsible for issuing RA-certificates to the LRA and Local Supporters
Responsible for ensuring key bearer tokens are available to the RA-personnel

3.2 LRA (Local RA)

This role is responsible for the following

- ID-proofing of physical persons (Certificate Holders that are End-Users)
- Issuing certificates
- Suspend certificates
- Revoking certificates
- Archiving of documents associated with the application or revocation process, e.g. applications, Terms and Conditions and revocations requests etc.

The LRA must be educated in the RA IT-system, how to do ID-proofing, what to do when something goes wrong, handling of its LRA-keys, handling of materials and equipment used and stored at an RA-office, how to enter/exit the RA-office properly, alarm procedures.

LRA responsibilities

ID proofing of individuals when applying for certificates
Archiving of certificate applications
Archiving of signed Terms and Conditions
Issuance and revocation of certificates
Archiving of results of certificate applications
Report identity theft to the correct authority (the police)

According to the four-eye principle, the same LRA person must never do the identity proofing of the applicant (applicant = a potential Certificate Holder) and the issuing of a certificate for the same applicant.

3.3 Local Supporter

The Local Supporter main task is to provide help to people who have problems with Samleikin, both before and when they have become Certificate Holders. Seen in a RA context they have the authority to suspend and unsuspend certificates for physical persons.

3.4 Internal auditor

This role is responsible for the following

- Peridoical and incident driven audits

At least an annual internal audit shall be carried out by the internal auditor. The result of the internal audit must reported to the Gjaldstovan TSP Management Board. Internal audits can also be ordered by the Gjaldstovan TSP Management Board in response to incidents or suspicions of malpractice within the RA organization.

The internal auditor will look to confirm compliance with this RAP and the RAPS, especially that:
• Documents, such as applications, Terms and Conditions etc, are stored appropriately
• LRA-keys are handled securely
• The roles (LRA manager, LRA and Local Supporters) are working in line with the RAPS
• Access to the RA facilities are controlled and managed appropriately
• Unused tokens (key-bearers) are stored safely and securely

4. RA persons and their keys/certificates

4.1 Certificate Life-Cycle of LRA-managers

The LRA manager must use a management CA certificate for LRA managers when handling their RA role within the RA organisation.

Gjaldstovan TSP Management Board shall perform identity proofing of the LRA manager and issue certificates according to documented internal procedures.

4.2 Certificate Life-Cycle of LRAs

The LRA must use a management CA certificate for RA persons when handling their RA role within the RA organisation.

The LRA manager shall perform identity proofing of the LRA and issue certificates to the LRA, see below.

4.2.1 Identity proofing process of LRA

4.2.1.1 Application for LRA-certificate

The potential LRA must:

- Meet physically at the RA facilities in person and apply for a certificate

4.2.1.2 Who can submit for a LRA-certificate?

These persons may submit a LRA-certificate applications:

- A physical person who is the subject of the certificate,
- Is a employee at the company, where the RA is affiliated or has a written agreement with the Gjaldstovan TSP Management Board to act as LRA.

- Must meet the requirments set forth in "Personnel controls" section in this RAP

4.2.1.3 Content of application

The LRA must inform the LRA Manager of the following information:

Full name

4.2.1.4 Approved documents for ID-proofing

A LRA person must prove his/her identity with one of the following ID-documents:

- Passports from the kingdom of Denmark.
- Driving license issued in the Faroe Islands or Denmark.

All documents submitted to RA by LRA must be original. There must be no information added, altered, overridden, and the like. The RAPS must describe how the authenticity of each ID document is proved.

The documents period of validity must not have expired.

If an LRA Manager has a doubt as to the identity of the potential LRA (e.g. a clear mismatch between the photograph in the personal document submitted and the applicants appearance or photograph), the registration shall be refused.

4.2.1.5 Performing identification and authentication

The LRA manager shall perform identification and authentication of all required LRA information according to the requirements below.

A certificate application must fulfill the following procedures:

1. The given information and the ID-documents are checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person
2. Application forms are archived.

4.2.1.6 Approval of LRA-certificate applications

The LRA Manager will approve an application for a LRA-certificate if the following criteria are met:

- Successful identification and authentication of all required LRA information and ID-documents.

4.2.1.7 Rejection of LRA-certificate applications

The LRA-manager will reject a LRA certificate application if:

- Identification and authentication of all required LRA information or ID-documents cannot be completed successfully

4.2.1.8 Certificate issuance

A LRA-certificate is created and issued following the approval of a LRA-certificate application by a following receipt of an LRA Manager request to issue the certificate. The LRA Manager creates and issues to a LRA-certificate applicant a LRA-certificate based on the information in a LRA-certificate application following approval of such LRA-certificate application.

The issuance of a certificate means that the issuing RA accepts the LRA application and the information that the LRA has declared.

The electronic registration by RAs shall be conducted in a it-system and in an environment that is secured from integrity flaws and follows routines that prevent faulty mixtures of LRA-keys and LRA information. The Gjaldstovan TSP has the responsibility for delivering and maintaining this it-system.

Every LRA-certificate application shall be traced back to the individual RA-person that signed the certificate application.

4.2.1.9 Activation data delivery to LRA

The LRA sets the activation data for the token bearing LRA certificate.

4.2.1.10 Certificate revocation

4.2.1.10.1 Circumstances for revocation

An LRA-manager shall revoke issued LRA-certificates under the following circumstances:

- If receiving a revocation request from either the LRA-Certificate Holder or an other LRA or a Local Supporter.
- If provided with information that a private key associated with a LRA-certificate is compromised or used by some entity that is not the LRA.
- If provided with information that the key bearer that contains the private key is no longer in use or possessed by the LRA

4.2.1.10.2 Revocation request handling

The LRA-manager must handle revocation request as quick as possible.

All revocation requests are archived along with the following information:

- How the request was received
- When the request was received
- The reason for revocation
- The result of successful revocation request
- A unique log-ID for the revocation request

4.2.1.10.3 Revocation request grace period

Revocation requests shall be submitted as promptly as possible within a reasonable time.

4.3 Certificate Life-Cycle of Local Supporters

The Local Supporters must use a management CA certificate for RA persons when handling their RA role within the RA organisation.

The LRA manager shall perform identity proofing of the Local Supporter and issue certificates to the Local Supporter, see below.

4.3.1 Identity proofing process of Local Supporters

4.3.1.1 Application for a Local Supporter certificate

The potential Local Supporter must:

- Meet physically at the RA facilities in person and apply for a certificate

4.3.1.2 Who can submit for a Local Supporter-certificate?

These persons may submit a certificate applications:

- A physical person who is the subject of the certificate
- Is a employee at the company, where the RA is affiliated or has a written agreement with the Gjaldstovan TSP Management Board to act as Local Supporter.
- Must meet the requirments set forth in "Personnel controls" section in this RAP

4.3.1.3 Content of application

The Local Supporter must inform the LRA Manager of the following information:

Full name

4.3.1.4 Approved documents for ID-proofing

A Local Supporter must prove his/her identity with one of the following ID-documents:

- Passports from the kingdom of Denmark.
- Driving license issued in the Faroe Islands or Denmark.

All documents submitted to RA by the Local Supporter must be original. There must be no information added, altered, overridden, and the like. The RAPS must describe how the authenticity of each ID document is proved.

The documents period of validity must not have expired.

If an LRA Manager has a doubt as to the identity of the potential Local Supporter (e.g. a clear mismatch between the photograph in the personal document submitted and the applicants appearance or photograph), the registration shall be refused.

4.3.1.5 Performing identification and authentication

The LRA manager shall perform identification and authentication of all required Local Supporter information according to the requirements below.

A certificate application must fulfill the following procedures:

1. The given information and the ID-documents are checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person
2. Application forms are archived.

4.3.1.6 Approval of Local Supporter-certificate applications

The LRA Manager will approve an application for a Local Supporter-certificate if the following criteria are met:

- Successful identification and authentication of all required Local Supporter information and ID-documents.

4.3.1.7 Rejection of Local Supporter certificate applications

The LRA-manager will reject a Local Supporter certificate application if:

- Identification and authentication of all required Local Supporter information or ID-documents cannot be completed successfully

4.3.1.8 Certificate issuance

A Local Supporter-certificate is created and issued following the approval of a Local Supporter-certificate application by a following receipt of an LRA Manager request to issue the certificate. The LRA Manager creates and issues to a Local Supporter-certificate applicant a Local Supporter-certificate based on the information in a Local Supporter-certificate application following approval of such Local Supporter-certificate application.

The issuance of a certificate means that the issuing RA accepts the Local Supporter application and the information that the Local Supporter has declared.

The electronic registration by RAs shall be conducted in a it-system and in an environment that is secured from integrity flaws and follows routines that prevent faulty mixtures of Local Supporter-keys and Local Supporter information. The Gjaldstovan TSP Management Board has the responsibility for delivering and maintaining this it-system.

Every Local Supporter-certificate application shall be traced back to the individual RA employee that signed the certificate application.

4.3.1.9 Activation data delivery to Local Supporters

The Local Supporter sets the activation data for the token bearing Local Supporter certificate.

4.3.1.10 Certificate revocation

4.3.1.10.1 Circumstances for revocation

An LRA-manager shall revoke issued Local Supporter-certificates under the following circumstances:

- If receiving a revocation request from either the Local Supporter-Certificate Holder or an other LRA or a Local Supporter.
- If provided with information that a private key associated with a Local Supporter-certificate is compromised or used by some entity that is not the L ocal Supporter.
- If provided with information that the key bearer that contains the private key is no longer in use or possessed by the Local Supporter

4.3.1.10.2 Revocation request handling

The LRA-manager must handle revocation request as quick as possible.

All revocation requests are archived along with the following information:

- How the request was received
- When the request was received
- The reason for revocation
- The result of successful revocation request
- A unique log-ID for the revocation request

4.3.1.10.3 Revocation request grace period

Revocation requests shall be submitted as promptly as possible within a reasonable time.

4.4 Certificate Life-Cycle of Internal Auditor certificates

The Internal Auditor must use a management CA certificate for Internal Auditors when handling their RA role within the RA organisation.

Gjaldstovan shall perform identity proofing of the Internal Auditor and issue certificates according to documented internal procedures.

5. Certificate Life-Cycle of physical persons (Certificate Holders that are End-Users)

5.1 Overall requirements:

The LRA Manager shall make sure that there are routines implemented regarding:

- ID-proofing of individuals when applying for certificates

- Archiving of certificate applications
- Issuance, suspension, revocation and renewal of certificates
- Archiving results of certificate applications

These routines shall be described in the RAPS of RAs.

According to the four-eye principle, the same LRA employee must never do the identity proofing of the applicant/Certificate Holder and the issuing of certificate to the same applicant/Certificate Holder.

(Applicant = a potential Certificate Holder).

LRAs shall issue certificates under the following circumstances:

- If a valid applicant submits a valid certificate application
- If the applicant information can be validated in accordance with the CP and the associated practice statement.
- If the applicant is in exclusive control of an approved key bearer for the certificate.

All certificate Applicants must undergo an enrollment process consisting of:

- Completing a certificate application and providing true and correct information
- Generating, or arranging to have generated, a key pair
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to the issuing CA

5.2 Application for certificate

5.2.1 Requirements regarding physical presence or equivalent

The applicant (a potential Certificate Holder) must either:

- Meet physically at the RA facilities in person and apply for a certificate or
- Apply for a certificate through a process that is equivalent to physical presence, e.g. online self-service.

5.2.2 Who can submit a certificate application

Entities that may submit certificate applications:

- A physical person who is the subject of the certificate, and
- Is a physical person at least 15 years old, and
- Possess a Faroese personal number (p-tal)

A physical person may be a citizen of the Faroe Islands or a foreigner as long as the person possess a Faroese personal number (p-tal).

5.2.3 Content of application

The Applicant must inform the RA of the following information:

Full name
P-tal (the faroese personal identification number)
Phone number
E-mail address

5.2.4 Approved documents for ID-proofing

A physical person must prove his/her identity with one of the following ID-documents:

- Passport issued by a public authority in the country of origin of the physical person.
- National driving license issued in the Faroe Islands or Denmark

If applications are conducted without the applicants physical presence, only the following personal photo ID-documents are permitted:

- Passport from the Kingdom of Denmark
- Danish/Faroese driving license issued in the Faroe Islands or Denmark

If applications are conducted without the applicants physical presence, the applicant must send in a photograph together with the ID-documents. The photograph and the ID document must be sent via an approved ID-verification software solution in the self-service registration application, that can ensure that the photograph was taken as part of the enrollment process.

All documents submitted to RA by applicants must be original. There must be no information added, altered, overridden, and the like. The RAPS must describe how the authenticity of each ID document is proved.

The documents period of validity must not have expired.

If non-danish (Kingdoms of Denmark, including faroese) passports are used, a copy of the passports must be archived together with the certificate application in the RA-system.

If an RA-person has a doubt as to the identity of the applicant (e.g. a clear mismatch between the photograph in the personal document submitted and the applicants appearance or photograph), the registration shall be refused.

5.2.5 Terms of use

All applicants must approve the Terms and Conditions before becoming Certificate Holder.

5.3 Certificate Application Processing

5.3.1 Performing identification and authentication functions

An LRA shall perform identification and authentication of all required applicant information according to the requirements below.

A certificate application must fulfill the following procedures:

1. The given information and the ID-documents are checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person
    a. The p-tal and name are checked against the Civil Registration System (FOLK)
    b. Passports from the kingdom of Denmark and Danish driving license are checked against the Danish passport register
    c. Faroese driving license are checked against the Faroese driving license register (koyrikortsskráin)
2. If the shown ID-document cannot be checked against neither the Danish passport register or the Faroese driving license register, extra steps must be taken to minimize the risk of identity theft,
    a. "Ekstra steps" methods accepted are:
        i. asking control question based on information in FOLK about the applicant, e.g. prior adresses, birthplace, name of children.
        ii. if FOLK only has limited information about the applicant e.g. if the applicant has only have been in Faroe Islands for a short while, then the applicant will need to bring an attesting witness
        iii. The attesting witness must be at least 18 years old, have a p-tal and must present valid ID document, and sign a solemn declaration (trú og heiður váttan) under penalty of law.
3. The LRA checks the application ensuring that all applicable Terms and Conditions are accepted.
4. Application forms are archived.

5.3.2 Approval of certificate applications

An LRA-person will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required applicant information and ID-documents.

5.3.3 Rejection of certificate applications

An LRA will reject a certificate application if:

- Identification and authentication of all required applicant information or ID-documents cannot be completed successfully
- The applicant fails to respond to notices within a specified time

5.3.4 Time to process certificate applications

RAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application.

A certificate application remains active until rejected.

5.4 Certificate issuance

5.4.1 RA actions during certificate issuance

A certificate is created and issued following the approval of a certificate application by a following receipt of an LRA-request to issue the certificate. The LRA creates and issues to a certificate applicant a certificate based on the information in a certificate application following approval of such certificate application.

The issuance of a certificate means that the issuing LRA accepts the applicants application and the applicants information that the applicant has declared.

The electronic registration by LRAs shall be conducted in a it-system and in an environment that is secured from integrity flaws and follows routines that prevent faulty mixtures of keys and Certificate Holder information. The Gjaldstovan TSP Management Board has the responsibility for delivering and maintaining this it-system.

Certificates shall be generated after an LRA first has ascertained that all application and control routines have been fulfilled.

Every certificate application from an LRA shall be traced back to the individual LRA that signed the certificate application.

5.5 Activation data delivery to Certificate Holders

5.5.1 Activation - token: Samleikin app - online registration

The applicant sets its own PIN on the Samleikin app.

5.5.2 Activation - token: Samleikin app - physical attendance

The applicant sets its own PIN on the Samleikin app.

5.5.3 Activation - token: Samleikin hardware token - physical attendance

The Applicant sets its own PIN on the Samleikin hardware token.

5.6 Certificate revocation

5.6.1 Circumstances for revocation

The main difference between suspension and revocation is, that the suspension is a deactivation of the certificate that can be unsuspended again, while a revocation can not be withdrawn.

An LRA shall revoke issued certificates under the following circumstances:

- If receiving a revocation request from either the Certificate Holder or an RA-employee (LRA manager, LRA or Local Supporter)
- If provided with information that a private key associated with a certificate is compromised or used by some entity that is not the Certificate Holder
- If provided with information that the key bearer that contains the private key is no longer in use or possessed by the Certificate Holder
- If provided with information that the Certificate Holder violates the Terms and Conditions.

5.6.2 Who can submit a revocation request

Revocation requests can be made by:

- LRA
- The Certificate Holder

5.6.3 Revocation request handling

When receiving a revocation request, the LRA must ensure that the identification is carried out in a way that ensures the identity of the person in the best possible way, for example by a combination of name, population registration address and e-mail address.

LRA shall ensure that the revocation request procedure, as far as possible, does not allow unauthorized revocations while allowing authorized revocations to be addressed by telephone, via email or online through the Samleikin website.

All revocation requests are archived along with the following information:

- How the request was received
- When the request was received
- The reason for revocation
- The result of successful revocation request
- A unique log-ID for the revocation request

5.6.4 Revocation request grace period

Revocation requests shall be submitted as promptly as possible within a reasonable time.

5.7 Certificate suspension

5.7.1 Circumstances for suspension

The main difference between suspension and revocation is, that the suspension is a deactivation of the certificate that can be unsuspend again, while a revocation can not be withdrawn.

An LRA or the Local Supporter shall suspend a issued certificates under the following circumstances:

- If receiving a suspension request from the Certificate Holder

5.7.2 Who can submit a suspension request

Suspension requests can be made by:

- Certificate Holder

5.7.3 Suspension request handling

When receiving a suspension request, the LRA or Local Supporter must ensure that the identification is carried out in a way that ensures the identity of the person in the best possible way, for example. by a combination of name, population registration address and e-mail address.

LRA or Local Supporter shall ensure that the suspension request procedure, as far as possible, does not allow unauthorized suspensions while allowing authorized suspensions to be addressed by telephone, via email or online through the Samleikin website.

All suspensions requests are archived along with the following information:

- How the suspension was received
- When the request was received
- The reason for suspension
- The result of successful suspension request
- A unique log-ID for the suspension request

5.7.4 Suspension request grace period

Revocation requests shall be submitted as promptly as possible within a reasonable time.

5.8 Certificate Derivation

Derivation is when the Certificate Holder moves the private key from on device to another.

It must be ensured that - taking into account the risks of a change in the person identification data - derivation of the certificate from one device to another meets the same assurance requirements as initial identity proofing and verification or is based on a valid certificate of the same, or higher, assurance level.

Derivation is permitted from:

- the device where the Certificate Holders Samleikin app is on and to another device in sole control of the Certificate Holder where the Samleikin app is on
- the Certificate Holders Samleikin hardware token to the device in sole control of the Certificate Holder where where Samleikin app is on

Derivation is not permitted from the Samleikin hardware token to another Samleikin hardware token.

5.9 Outlined processes

The RA must have outlined processes in place in the RAPS that meet the requirements in this RAP and relevant articles in the eIDAS implementing Act 2015/1502 level of assurance Substantial.

There must be outlined processes for:

5.9.1 The enrollment process

5.9.1.1 Requirements regarding the application and registration

The LRA must:

1. Ensure the applicant is aware of the terms and conditions in the Terms and Conditions related to the use of the certificate.
2. Ensure the applicant is aware of recommended security precautions related to the certificate.
3. To collect the relevant identity data required for identity proofing and verification.

5.9.1.2 Requirements regarding identity proofing and verification

The LRA must:

1. Ensure that the person has been verified to be in possession of a approved ID-document
2. Ensure that the ID-document is checked to determine that it is genuine; or, according to an authoritative source, it is valid and it is known to exist and relates to a real person
3. Ensure that steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired ID-documents;

5.9.2 Certificate management processes

5.9.2.1 Issuance, delivery and activation

The LRA must:

Ensure that after issuance, the certificate is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.

5.9.2.2 Suspension, revocation and unsuspension

The LRA or Local Supporter must:

1. Ensure it is possible to suspend and/or revoke the certificate in a timely and effective manner.
2. Ensure that measures are taken to prevent unauthorised revocation and unsuspension .
3. Ensure that unsuspension only takes place if the same assurance requirements as established before the revocation continue to be met.

5.9.2.3 Renewal and replacement

Certificate renewal means according to RFC 3647 the issuance of a new certificate without changing the Key-pair. Samleikin does not support certificate renewal for end entity (non-CA) certificates or CA-certificates.

The RAP and RAPS however talk about renewal. But it is actually not renewal according to RFC 3647, but a new application because it is the issuance of a new certificate with a new Key-pair. To confuse the end-user as little as possible it is however called renewal in the RAP and RAPS, because of the different user experience.

The LRA or Local Supporter must:

Ensure that - taking into account the risks of a change in the person identification data - renewal of the certificate needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid certificate of the same, or higher, assurance level.

5.9.3 Compliance and audit processes

The Gjaldstovan TSP Management Board must:

Ensure the existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with this RAP.

6. Records archival

Records archival shall adhere to the CP and associated practice statements. The implementation of the requirements stated in the CP and associated practice statements shall be described in the RAPS of RAs.

The following specific archival requirements apply for each RA:

- Certificate applications
- Non-danish passports used for ID-proofing
- Suspension and revocation request
- Archiving of applicant validations, including ID-proofing
- Archiving of results of certificate applications
- All registration information including the following shall be recorded:
    - Type of document(s) presented by the applicant to support registration
    - Record of unique identification data, numbers, or a combination thereof of identification documents, if applicable
    - Storage location of copies of applications, including the signed Terms and Conditions
    - Identity of entity accepting the application
    - Method used to validate identification documents

7. Compromise and disaster recovery

Every RA within Samleikin is responsible for developing and implementing its local compromise and disaster recovery plans. The RAPS of each RA shall contain a reference to such compromise and disaster recovery plans.

8. RA termination

In the event a RA is terminated from Samleikin, the RA is obligated to fulfill the following procedures:

- Inform relevant parties, that the RA has a relation with, at least 3 months before termination.
- Terminate all permissions that are held by RA employees.
- Ensure that all archived information and logs are kept for the entire duration of the archival period and handed over to the Gjaldstovan TSP Management Board upon termination.

The requirements identified in ETSI EN 319 401, clause 7.12, shall apply. In addition the following particular requirements apply:

- Regarding the requirement REQ-7.12-06 of clause 7.12 of ETSI EN 319 401, this shall apply to registration information, revocation status information and event log archives for their respective period of time as indicated to the Certificate Holder and relying party.
- Regarding the requirement REQ-7.12-10 of clause 7.12 of ETSI EN 319 401, this shall also include the handling of the revocation status for unexpired certificates that have been issued.

An RA within Samleikin must provide guarantees and insurances that the necessary means are available to fulfill the above requirements in a termination situation.

9. Facility, management, and operational controls

9.1 Physical controls

Physical controls refer to the physical protection of sites, equipment and information that are related to an RA-office. The goals of physical controls are to prevent unauthorized physical access, damage and disruptions. These controls must be related to the risks and threats that RAs within Samleikin are subject to. The Gjaldstovan TSP Management Board together with the RA must continuesly conduct risk analysis related to the risks concering the RA. Pro cedures for physical controls shall be documented in the RAPS of RAs.

The requirements for physical controls at the RA-office are:

- The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.
- Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.
- It must be a location that is under exclusive control of the RA, this also applies to the equipment used and stored in the RA-office.
- Secure storage of certain equipment when not in use or before issuance, including RA-stations, hardware tokens about to be issued, any RA-procedures deemed secret/semi-secret.
- Video monitoring of the RA-locations entry and exit.
- Locks and doors of sufficient quality for all entry/exits to the location.
- Means to physically isolate citizens from RA-personnel and RA-equipment (for every physical visit to the RA-office by non-RA-persons).
- Means to protect equipment and cables from illicit tampering.
- Sufficient and reliable power for all equipment.
- A solid plan and guideslines for how to do controlled evacuation in case of threats, fire, and other emergency situations without exposing more than necessary of the RA-location and its assets. Every RA persons must be in possession (either on paper or digitally) of this plan and guideslines.
- Controls shall be implemented to protect against equipment, information, media and software relating to the RA-systems being taken off-site without authorization.

9.1.1 Protection of RA private keys

Every RA employee has the responsibility for its own personal RA private key. When not at work the RA employee must keep the RA private key safe and in sole control.

If the RA employee knows or suspects that the RA private key:

- has been compromised or used by some entity that is not the RA employee,
- is no longer possessed by the RA person

or others similar situation to those above, the RA employee must without any hesitation submit a revocation request to the LRA manager.

9.2 Personnel controls

The personnel controls contain sensitive information and are only available to anyone after explicit agreement with the Gjaldstovan TSP Management Board. An overview of the personnel control requirements is described in the subsections following.

9.2.1 Qualifications, experience, and clearance requirements

RAs shall require that all (potential) RA personnel present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily. A person within an RA organization shall not have other roles that can be in conflict with the assignment in the RA organization.

9.2.2 Background check procedures

RA-personnel shall meet the requirements of the RA background check procedures. These procedures shall be documented in the RAPS of RAs.

The RA organization shall conduct background checks of RAs personnel. This includes:

- A confirmation of previous employments
- A check of professional references
- A confirmation of the highest or most relevant educational degree obtained
- A search of criminal records

9.2.3 Training requirements

LRA managers shall provide and document attendance for their personnel with the requisite training needed for their personnel to perform their job responsibilities relating to RA-operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel.

Training programs must address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of every tool/procedure used by RA-personnel
- Hardware and software in use
- All duties the person is expected to perform
- Incident and compromise reporting and handling
- Disaster recovery and business continuity procedures

9.2.4 Retraining frequency requirements

RAs shall provide and document attentance refresher training and updates at least every year to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

9.2.5 Job rotation frequency and sequence

No stipulations.

9.2.6 Sanctions for unauthorized actions

If the RA as a whole does not act in accordance with this RAP or the RAPS the sanctions are determined by the Gjaldstovan TSP Management Board from case to case.

If an RA employee does not act in accordance with this RAP or the RAPS sanctions are determined by the LRA Manager and stated in the RAPS.

9.2.7 Independent contractor requirements

Independant contractors are not allowed in Samleikin RA organizations.

9.2.8 Documentation supplied to personnel

Every RA employee must access to the following material:

- RAPS
- Plan and guideslines for how to do controlled evacuation in case of threats, fire, and other emergency situations
- Lock-down procedure

9.3. Computer security controls

Computer security technical requirements

RA functions shall only take place on trustworthy systems. The RA shall ensure that the systems executing RA-software and data files are secure from unauthorized access.

The RA shall have networks separated from other entities. This separation shall prevent illicit network access except for only permitted traffic flows. The RA-environments shall use firewalls to protect from illicit internal and external traffic and limit the nature and source of network activities that may access RA-systems.

Access to the RA-environment shall be limited to trusted persons having a validated reason for such access.

RAs shall ensure that the systems maintaining RA-software and data files are trustworthy systems secure from unauthorized access.

RAs shall separate access to RA-systems and its information from other components. This separation shall prevent access except through defined processes. RAs shall also have mechanisms and policies in place to control and monitor the configuration of RA-systems. Upon installation, and at least once a day, processing centers shall validate the integrity of the RA-system.

Software and hardware features that are not used by RAs shall be deactivated.

9.4 Computer security rating

The Gjaldstovan TSP Management Board selects and delivers the RA system. The RA system is part of Samleikin core systems and must comply to all relevant demands and will be audited as a trustworthy system in the Samleikin PKI.

10. Compliance audit and other assessments of RAs

Two kinds of RA audits shall be implemented:

- External audit – Audits the implementation of the requirements is performed by external auditor in accordance with the stipulations in the certificate policies NCP and NCP+ and their associated practice statements. RA must give access to external auditors in cooperation with the Gjaldstovan TSP Management Board.
- Internal audit – The implementation of the RAPS associated with an RA operating boundary and the compliance with this RAP is performed by the internal auditor associated with the RA organization. Each RA shall describe how such audits are handled and conducted in its RAPS.